PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) **Classification internationale des brevets** [7] : G11B 20/00, 23/28

A1

(11) **Numéro de publication internationale:** **WO 00/51119**

(43) **Date de publication internationale:** 31 août 2000 (31.08.00)

(21) **Numéro de la demande internationale:** PCT/FR00/00483

(22) **Date de dépôt international:** 25 février 2000 (25.02.00)

(30) **Données relatives à la priorité:**
99/02474 26 février 1999 (26.02.99) FR

(71) **Déposant** *(pour tous les Etats désignés sauf US)*: SCHLUMBERGER SYSTEMES [FR/FR]; 50, avenue Jean Jaurès, F-92120 Montrouge (FR).

(71)(72) **Déposant et inventeur:** FAUSSE, Arnaud [FR/FR]; 11bis, rue de Maubeuge, F-75009 Paris (FR).

(74) **Mandataire:** UTZMANN-NORTH, Anne; Schlumberger Systèmes, Test & Transactions, 50 Avenue Jean Jaurès, Boîte postale 620-12, F-92542 Montrouge Cedex (FR).

(81) **Etats désignés:** CN, JP, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) **Title:** SECURE OPTICAL DISK AND METHOD FOR SECUREMENT OF AN OPTICAL DISK

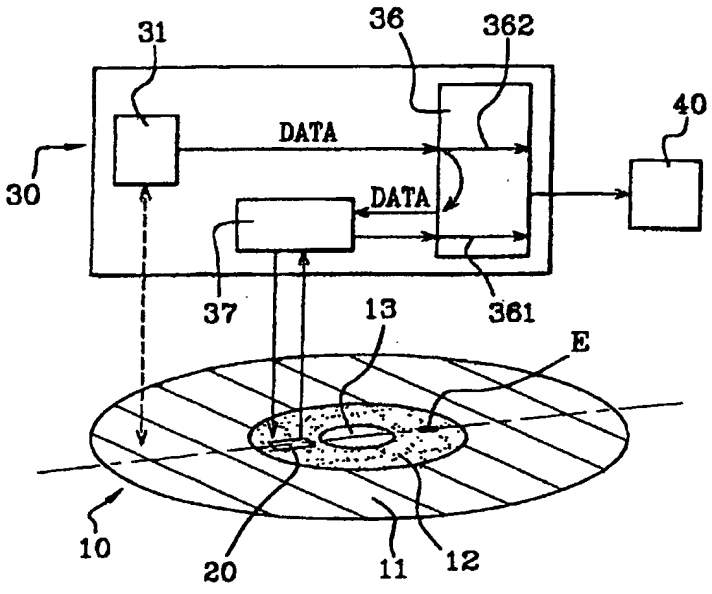
(54) **Titre:** DISQUE OPTIQUE SECURISE ET PROCEDE DE SECURISATION D'UN DISQUE OPTIQUE

(57) **Abstract**

The invention relates to a secure optical disk for storing data. The invention also relates to a method for securement of such a disk. The invention is characterized in that said disk comprises a portable object that is provided with a memory consisting of at least one secret key, in addition to means for exchanging data, whereby said key is used to decrypt data from said disk while remaining in the portable object and the means for exchanging data are used to exchange data between the portable object and the disk. The invention is particularly suitable for use with CD-ROMs.

(57) **Abrégé**

L'invention concerne un disque optique sécurisé de stockage de données. Elle concerne également un procédé de sécurisation d'un tel disque. L'invention se caractérise en ce que ledit disque comporte, d'une part, un objet portatif comportant une mémoire comprenant au moins une clef secrète, et, d'autre part, des moyens d'échange de données, ladite clef permettant de décrypter des données dudit disque tout en demeurant dans ledit objet portatif, lesdits moyens d'échange permettant d'échanger lesdites données entre ledit objet portatif et ledit disque. L'invention s'applique, en particulier, aux CD-ROM.



UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

DISQUE OPTIQUE SECURISE ET PROCEDE DE SECURISATION D'UN DISQUE OPTIQUE

La présente invention concerne un disque optique de stockage de données. Elle concerne également un procédé de sécurisation d'un tel disque.

L'invention trouve une application particulièrement avantageuse dans des domaines tels que les domaines de l'informatique, des jeux, de l'audiovisuel.... Les médias de stockage de données, notamment les disques optiques, comprennent des données destinées à être exploitées généralement sur un terminal tel qu'un ordinateur ou un moniteur de télévision. Lesdites données sont des informations de type texte, des images, du son ou encore des logiciels.

De nombreuses copies frauduleuses des données contenues dans lesdits médias sont effectuées au moyen de logiciels accessibles à tous. Ces logiciels permettent de dupliquer des données d'un média en dépit des droits d'auteurs qui protègent généralement lesdites données. Un dispositif connu de l'état de l'art propose d'utiliser un boîtier de sécurité pour empêcher les copies pirates des données contenues dans un média. Le boîtier qui contient un circuit électronique d'identification est relié par exemple à un ordinateur dans lequel est introduit ledit média. Ledit dispositif divulgue la présence d'un programme dans le média permettant d'identifier le boîtier de sécurité par l'intermédiaire dudit circuit électronique. Le programme est chargé dans l'ordinateur puis il effectue l'identification. En cas d'absence du boîtier approprié, les données ne peuvent être lues, par suite, le média ne peut être utilisé. Le dispositif n'offre qu'une sécurité minimale dans la mesure où le programme de vérification peut être neutralisé sur l'ordinateur. Il n'existe alors plus aucune protection. De plus, généralement, un boîtier de sécurité est associé à un seul média. Par suite, la gestion de la

sécurité devient très onéreuse et compliquée puisqu'il faut un nouveau boîtier de sécurité pour tout nouveau média.

Aussi un problème technique à résoudre par l'objet de la présente invention est de proposer un disque optique sécurisé de stockage de données, ainsi qu'un procédé de sécurisation d'un tel disque, qui permettent d'éviter les copies frauduleuses des données contenues dans lesdits disques tout en n'alourdissant pas l'utilisation desdits disques.

Une solution au problème technique posé se caractérise, selon un premier objet de la présente invention, en ce que ledit disque optique sécurisé de stockage de données, caractérisé en ce qu'il comporte, d'une part, un objet portatif comportant une mémoire comprenant au moins une clef secrète, et, d'autre part, des moyens d'échange de données, ladite clef permettant de décrypter des données dudit disque en demeurant dans ledit objet portatif, lesdits moyens d'échange permettant d'échanger lesdites données entre ledit objet portatif et ledit disque.

Selon la présente invention, un procédé de sécurisation d'un disque optique est remarquable en ce que le procédé comporte les étapes consistant à :

- on décrypte des données dudit disque au moyen d'une clef secrète comprise dans une mémoire d'un objet portatif intégré audit disque et demeurant dans ledit objet lors du décryptage,
- on échange les données dudit disque entre ledit objet portatif et ledit disque grâce à des moyens d'échange de données intégrés audit disque.

Ainsi, comme on le verra en détail plus loin, le dispositif de l'invention permet de protéger des données du média en les cryptant et d'empêcher ainsi une lecture en clair des données. Une copie des données est inutilisable puisque lesdites données sont cryptées. Pour effectuer une lecture desdites données, ces dernières doivent être au

préalable décryptées au moyen d'une clef secrète comprise dans ledit objet, lequel est intégré dans le média de stockage de données. La clef secrète est préférentiellement unique à un média. Ainsi, une lecture en clair de données est uniquement possible à partir dudit média.

La description qui va suivre au regard des dessins annexés, donnés à titre d'exemples non limitatifs, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

La figure 1 est une vue de dessus d'un média de stockage conforme à l'invention.

La figure 2 est un schéma d'un objet portatif compris dans le média de la figure 1.

La figure 3 est une vue de côté d'un lecteur de média et du média de la figure 1.

La figure 4 est un schéma logique du lecteur de média de la figure 3.

La figure 5 est un autre schéma logique du lecteur de média de la figure 3.

La figure 6 est une vue partielle en perspective du lecteur de média de la figure 3.

La figure 7 est une vue de dessus d'une première réalisation du média de la figure 1.

La figure 8 est une vue de dessus d'une seconde réalisation du média de la figure 1.

La figure 9 est une vue de dessus partielle du lecteur de média de la figure 3.

La figure 10 est un schéma de données provenant du média de la figure 1.

La figure 11 est un autre schéma de données provenant du média de la figure 1.

Sur la figure 1 est représenté un média 10 de stockage de données. Ledit média intègre un objet portatif 20 et des moyens d'échange de données. Le média 10 comporte trois zones principales. La zone périphérique 11 permet de stocker des données. Les deux autres zones sont des zones centrales. L'une est un trou 13 placé au centre du média et dans lequel un axe mécanique peut se glisser, ladite zone correspond ainsi à un axe de rotation. L'autre est une zone neutre 12 placée entre le trou 13 et la zone périphérique 11 et ne contenant aucune donnée. Ledit objet portatif 20 est intégré dans une zone centrale dudit média 10 qui est la zone neutre 12. Comme le montre la figure 2, l'objet portatif 20 comprend une mémoire 22 et un bloc de contacts 23 permettant d'établir des contacts électriques avec par exemple un terminal. La mémoire 22 comprend une clef K1 secrète. Cette clef est préférentiellement unique pour chaque média, c'est à dire qu'elle n'a pas de doublet, ni dans le média auquel elle appartient, ni dans d'autres médias. Ledit objet portatif 20 comprend un cryptoprocesseur 21. Ledit objet portatif est une puce à circuit intégré. Une puce est sécurisée.

Ledit média 10 est un disque optique. Un disque optique est un disque composé de pistes comportant des données. Lesdites données comprennent un logiciel d'application tels que par exemple un logiciel de jeu vidéo ou d'exploitation de bases de données.

La suite du présent exposé de l'invention a trait à l'exemple des CD-ROM. Néanmoins, il est bien entendu que l'invention s'applique de manière générale à tout autre disque optique.

Dans le cas d'un CD-ROM, les données d'une piste sont formatées suivant des standards tels que ceux appelés Livre Jaune et Livre Vert définis par Philips. Les standards définissent essentiellement deux modes de formatage de données. Suivant un premier mode appelé mode 1, la piste comporte des données utilisateurs, des données d'entête et

des données de détection d'erreurs permettant d'avoir deux niveaux de détection d'erreurs. Suivant un deuxième mode appelé mode 2, la piste comporte des données utilisateurs, des données d'entête et des données de détection d'erreurs permettant d'avoir un seul niveau de détection d'erreurs. Les données d'entête comprennent un numéro de piste et des indicateurs de début et fin de piste. Les données utilisateurs comprennent le logiciel d'application.

Le média 10 connaît trois grandes phases. Une phase de fabrication, une phase dite de gravure-personnalisation et une phase d'utilisation.

Lors de la phase de fabrication, on place le média 10 sur une machine de fraisage qui réalise un logement dans lequel on intègre l'objet portatif 20. Ledit objet est inséré et collé dans le logement. Cependant, le poids dudit objet portatif peut déséquilibrer ledit média 10. Afin d'éviter ce problème, on prévoit que ledit média 10 comporte des moyens E d'équilibrage permettant d'équilibrer ledit média en le replaçant son centre de gravité sur son axe de rotation. Un mode de réalisation non limitatif desdits moyens d'équilibrage se fera au moyen d'une masselotte d'équilibrage composée d'une rondelle de métal collée dans un fraisage effectué dans ledit média, ladite masselotte étant diamétralement opposée audit objet portatif 20 du média 10, comme le montre la figure 1. La phase de fabrication est terminée.

Lors de la phase de gravure-personnalisation, des données sont cryptées et inscrites dans le média 10. Le cryptage et l'inscription, appelée aussi gravage, se font au moyen d'une machine de gravage. On prévoit que ladite machine de gravage est composée essentiellement des éléments suivants :

- une sonde munie de contacts permettant un échange de données entre un ordinateur pilotant ladite machine et l'objet portatif 20 intégré du média 10,

- un cryptoprocesseur représentant un algorithme de cryptage, permettant de crypter des données à graver,
- un logiciel générateur de clefs secrètes,
- un logiciel de chargement de clefs secrètes dans l'objet portatif 20 du média 10.

La phase de gravure-personnalisation se déroule selon les étapes suivantes :

- on charge un média 10 vierge,
- on génère un jeu individuel de clefs secrètes,
- on détermine les données à crypter,
- on crypte les données au moyen d'une clef K1 secrète unique,
- on inscrit lesdites données cryptées dans ledit média 10 ainsi que les données non cryptées,
- on charge le jeu individuel de clefs secrètes dans l'objet portatif 20 du média 10.

La clef K1 secrète unique provient du jeu individuel de clefs généré. Ladite clef K1 est soit l'une des clefs du jeu de clefs, soit une combinaison de clefs dudit jeu. Afin d'avoir une gestion optimisée des clefs et des médias associés, plusieurs clefs ou jeux de clefs peuvent provenir d'une même clef, par exemple, lorsqu'on diversifie des clefs à partir d'une clef appelée clef « maître ». De même, pour faciliter la gestion des médias, on pourra utiliser une même clef secrète pour une série de médias reconnaissables, par exemple, par un numéro de série.

On peut choisir de crypter toutes les données du média ou seulement une partie. Une piste comporte des blocs de données de deux mille quarante huit octets. Les données sont cryptées par groupe de huit octets si on utilise un algorithme de cryptage tel que le DES. D'autres algorithmes symétriques de cryptage peuvent être utilisés. L'ensemble des données est gravé dans la zone périphérique 11 du

média. Le gravage se fait par des procédés connus tels que les procédés de type magnéto-optique ou brûlage de colorant par laser.

Désormais, le média 10 peut être utilisé.

Lors de la phase d'utilisation, dans une première étape, on lit les données qui se trouvent dans le média 10. La lecture se fait au moyen d'un lecteur 30 de média. Comme le montrent les figures 3 et 4, le lecteur est composé essentiellement d'un plateau 35 dans lequel vient se loger le média 10, d'un moteur M permettant de faire tourner le média 10, d'un axe 32 mécanique qui vient se glisser dans le trou 13 du média 10, de deux plaques 33 et 34, permettant de maintenir le média 10 stable lorsque le lecteur fonctionne, d'une tête 31 de lecture laser comportant notamment une diode laser et des photodétecteurs, la diode laser permettant d'obtenir un faisceau laser, d'une interface 36 de type standard IDE ou SCSI permettant de connecter ledit lecteur 30 à un ordinateur 40, et, d'une interface 37 cryptoprocesseur permettant un dialogue avec le cryptoprocesseur 21 de l'objet portatif 20. La plaque 34 est appelée poupée et est solidaire de l'axe 32.

La lecture se fait de manière optique avec le faisceau laser et est définie dans des standards appelés tel que le Livre Bleu édité par Philips. Elle se fait suivant un procédé qui s'appuie sur la détection de la réflexion d'un faisceau laser sur une piste tantôt réfléchissante tantôt absorbante définissant ainsi des données se présentant sous forme de lumière. Le faisceau laser est par la suite dirigé vers les photodétecteurs qui sont des transducteurs permettant une conversion de la lumière en signaux électriques. Lesdits signaux électriques sont traités à un premier niveau afin d'éliminer des erreurs de discordance lors d'une lecture de données. La piste est par suite reconstituée, puis un code correcteur de deuxième niveau est appliqué lorsque celle-ci est formatée avec le mode 1. Par la suite, ladite piste est envoyée à l'interface 36 dudit lecteur 30 de média.

Le média 10 ainsi que le lecteur 30 de média ne comportent aucune indication permettant de dissocier les données cryptées des données non cryptées d'une piste. Ceci permet d'éviter une fraude qui consisterait à copier les indications portant sur un mode de cryptage des données contenues dans le média 10.

Dans une deuxième étape, le lecteur 30 de média reconnaît si le média 10 est équipé d'un cryptoprocesseur. A cette fin, il envoie la piste lue, via son interface 37 cryptoprocesseur, au média 10. Dans le cas où des données sont renvoyées par ledit média via un premier canal 361 de communication ouvert au préalable lors de la lecture dudit média 10, ledit canal étant compris dans l'interface 36, le lecteur 30 conclura à la présence d'un média 10 comportant un objet portatif 20 composé d'un cryptoprocesseur 21. Dans le cas contraire, aucune donnée n'est renvoyée, par conséquent, le média 10, ne contient aucun cryptoprocesseur et la lecture des données se fait sans décryptage.

Dans une troisième étape, dans le cas où le média 10 est équipé d'un cryptoprocesseur, comme le montre la figure 4, les données DATA lues sont envoyées à l'ordinateur 40 relié audit lecteur 30, via un deuxième canal 362 de communication ouvert au préalable lors de la lecture dudit média 10, ledit canal étant compris dans l'interface 36. Ces données sont appelées données brutes car elles ne subissent aucune modification. Dans le même temps, on envoie les données DATA lues au cryptoprocesseur 21. Selon un premier moyen de réalisation, on envoie lesdites données DATA, via l'interface 37 cryptoprocesseur. Ainsi, avant d'être envoyées au cryptoprocesseur, les données DATA sont modifiées au préalable en un format compréhensible par le cryptoprocesseur, par exemple en octets, grâce à l'interface cryptoprocesseur 37 comprise dans le lecteur de disque optique.

Selon un deuxième moyen de réalisation, comme le montre la figure 5, on envoie, au cryptoprocesseur 21 de l'objet portatif 20,

lesdites données DATA au moyen d'un bus 38 de liaison série universelle appelée USB, ledit bus étant intégré dans l'ordinateur 40. Par suite, un unique canal de communication compris dans l'interface 36 du lecteur 30 est nécessaire. Les données décryptées dans ledit cryptoprocesseur 21 sont, par la suite, renvoyées à l'ordinateur 40 via ce même bus 38. Dans ce cas, c'est l'ordinateur 40 qui comporte une interface cryptoprocesseur qui modifie les données DATA en un format compréhensible par le cryptoprocesseur.

On notera que ce mode de réalisation est utilisable également lors de la deuxième étape décrite précédemment.

Lors de l'envoi des données DATA lues audit cryptoprocesseur, on transfère les signaux électriques correspondants auxdites données, du lecteur 30 de média au média 10, et, du média 10 à l'objet portatif 20, grâce aux moyens d'échange de données intégrés audit média et à des moyens d'échange intégrés au lecteur 30 de média.

Soit, les moyens d'échange de données intégrés audit média 10 sont avec contacts, soit, les moyens d'échange de données intégrés audit média 10 sont sans contacts.

Dans le cas de moyens d'échange de données sans contacts, selon un mode de réalisation non limitatif de l'invention, les moyens d'échange de données intégrés audit média 10 sont une antenne. Les moyens d'échange de données intégrés au lecteur 30 sont une seconde antenne. Dans ce cas, les données sont échangées par couplage inductif entre lesdites première et seconde antennes.

Dans le cas de moyens d'échange de données avec contacts, selon un premier mode de réalisation non limitatif de l'invention, comme le montre la figure 6, des premiers moyens IN_B, OUT_B, VCC_B et GRD_B d'échange sont intégrés au lecteur 30 de média au niveau de l'axe 32 et de la poupée 34, et, comme le montre la figure 7 et les moyens IN_A, OUT_A, VCC_A et GRD_A d'échange de données sont

intégrés au média 10 au niveau d'une zone centrale qui est la zone neutre 12. Lorsque la poupée 34 est en contact avec le média 10, Les premiers moyens entrent en contact respectivement avec les deuxièmes moyens. Cela permet d'échanger des données entre ledit lecteur de média et ledit média. En outre, les deuxièmes moyens IN_A, OUT_A, VCC_A et GRD_A intégrés au média 10, sont reliés au bloc 23 de contacts de l'objet portatif 20 en des points de contact respectifs I, O, V et G. Lesdits deuxièmes moyens IN_A, OUT_A, VCC_A et GRD_A permettent également un échange de données entre ledit média 10 et ledit objet portatif 20. Ainsi, lesdits moyens d'échange de données, intégrés au média 10 et au lecteur 30, comprennent des moyens d'échange d'entrée IN_A, IN_B, des moyens d'échange de sortie OUT_A, OUT_B, des moyens VCC_A, VCC_B d'alimentation et des moyens GRD_A, GRD_B de mise à la masse.

Les moyens d'échange d'entrée IN_A et IN_B permettent de transporter des données du lecteur de média via le média 10. Le point de contact I et le moyen d'entrée IN_A permettent de transmettre les données du média 10 vers l'objet portatif 20. Les moyens d'échange de sortie OUT_A et OUT_B permettent de transporter des données du média 10 via le lecteur 30 de média. Le point de contact O et le moyen de sortie OUT_A permettent de transmettre les données de l'objet portatif 20 vers le média 10. Les moyens VCC_A et VCC_B d'alimentation permettent d'alimenter en tension ledit objet 20 portatif et les moyens GRD_A et GRD_B de mise à la masse permettent une mise à la masse dudit objet portatif.

Selon un second mode de réalisation, les moyens d'échange d'entrée IN_A, IN_B et de sortie OUT_A, OUT_B de données peuvent être confondus et être ainsi des moyens d'échange bidirectionnels.

On notera que selon un autre mode de réalisation, les premiers moyens IN_B, OUT_B, VCC_B et GRD_B d'échange de données intégrés

au lecteur 30 de média peuvent être intégrés au niveau de la plaque inférieure 33 du lecteur.

Pour permettre un transport efficace des signaux électriques, les moyens d'échanges de données précités intégrés audit média 10 sont composés d'un matériau permettant une bonne conductivité et évitant une trop grande oxydation desdits moyens. Ainsi, ils sont composés d'or. Lesdits moyens peuvent, par exemple, être des anneaux comme le montre la figure 7, des fils ou encore des arcs de cercles comme le montre la figure 8. Il en est de même avec les moyens d'échange de données intégrés au lecteur 30 de média. Préférentiellement, afin d'éviter la présence d'une boucle sensible au rayonnement électromagnétique et par suite d'éviter des parasites dus à ce rayonnement, les moyens d'échanges de données intégrés audit média 10 sont des arcs de cercle formant un secteur circulaire d'angle BETA et les moyens d'échange de données du lecteur 30 sont des arcs de cercle espacés d'un angle ALPHA inférieur à l'angle BETA, comme le montre la figure 9. Les arcs de cercles du média 10 et du lecteur 30 sont de même largeur W et sont distants d'une même largeur L. On garantit ainsi un contact permanent entre les différents moyens d'échange de données.

Après que les signaux électriques correspondants aux données DATA lues sont transmis à l'objet portatif 20 grâce aux moyens d'échanges de données définis précédemment, les données DATA sont décryptées au moyen d'un cryptoprocesseur qui les décrypte au moyen de la clef K1 secrète unique comprise dans la mémoire 22 de l'objet 20 portatif. Grâce à ce système de clef unique intégrée dans un objet portatif, une copie des données du média 10 sur un deuxième média, comportant ou non un cryptoprocesseur, est inutilisable.

Ledit cryptoprocesseur représente un algorithme inverse de celui qui a été utilisé pour crypter lesdites données. Ledit cryptoprocesseur est programmé ou câblé.

Selon un premier mode de réalisation non limitatif, ledit cryptoprocesseur est intégré audit objet portatif 20. La clef secrète K1 ne sort pas de la puce : elle y demeure. Selon un deuxième mode de réalisation, le cryptoprocesseur est un cryptoprocesseur rattaché au lecteur 30 de média. Dans ce deuxième mode de réalisation, il faut envoyer la clef K1 secrète de l'objet portatif 20 dans le lecteur de façon temporaire, le temps de décrypter les données DATA lues. Il est clair que dans ce cas il n'est nul besoin d'envoyer les données DATA à l'objet portatif 20. Cependant, on préférera le premier mode de réalisation qui est beaucoup plus sécuritaire étant donné que la clef K1 secrète demeure dans l'objet portatif 20, elle n'est jamais transmise à l'extérieur et n'est ainsi pas sujette à des fraudes qui consisterait à espionner le lecteur 30 de média pour reconstituer ladite clef K1 secrète. De plus, le fait que le cryptoprocesseur soit dans l'objet portatif empêche à un fraudeur de copier les moyens permettant de crypter ou décrypter.

Dans le cryptoprocesseur, les données DATA sont décryptées systématiquement, qu'elles soient à l'origine cryptées ou non, puis, le cas échéant, renvoyées audit lecteur 30, et enfin, transmises à l'ordinateur 40, via le premier canal 361 de communication si l'interface 37 cryptoprocesseur est utilisé.

On charge, de manière alternative, dans une mémoire 41 de l'ordinateur 40, les données DATA dudit média 10, brutes et décryptées. L'ordinateur pourra ainsi repérer les différents ensembles de données envoyés. Comme le montre la figure 10, les données B dites brutes et décryptées D, sont envoyées à l'ordinateur 40, préférentiellement, par pistes ou blocs complets, ou octets. On notera que les données non cryptées à l'origine, mais décryptées via le cryptoprocesseur 21 ne sont pas utiles. Cependant, le fait que le lecteur 30 délivre systématiquement à l'ordinateur 40 les données brutes et décryptées permet de se prémunir d'une attaque qui consisterait, d'une part, à différencier les

données cryptées et non cryptées, et, d'autre part, à trouver une manière de les utiliser, en se connectant tout simplement à la sortie du lecteur 30 de média.

Dans une quatrième étape, les données envoyées et chargées dans la mémoire 41 de l'ordinateur 40 sont utilisées de la manière suivante : lesdites données, qui comprennent le logiciel d'application du média 10, sont composées d'un couple de pistes ou blocs, une piste ou un bloc B1 dit brut et une piste ou un bloc D1 dit décrypté ayant pour même origine une piste ou un bloc O1 de données lues dans le média 10. La figure 10 montre un bloc B1 brut qui est composé, d'une part, de zones Ba de données non cryptées, appelées zones utiles, et, d'autre part, de zones Bb de données cryptées inutilisables. Le bloc D1 décrypté est composé de zones Db de données décryptées inutilisables et de zones Da, appelées également zones utiles, de données décryptées correspondant aux zones Bb de données cryptées du bloc B1 brut.

Le logiciel d'application comprend, d'une part, un programme d'autodémarrage reconnu par l'ordinateur, qui permet d'initialiser ledit logiciel, et, d'autre part, du code exécutable. Ledit code exécutable comprend un ensemble de liens permettant de relier différentes zones entre elles, de charger de nouvelles données en mémoire, de reconstituer une zone de données. Ledit programme d'autodémarrage est chargé initialement dans l'ordinateur 40.

Les zones utiles des différents blocs comportent généralement, d'une part, une partie du code exécutable, et, d'autre part, des données d'application utilisées par le logiciel d'application telles que par exemple des images, du texte, du son.

Comme le montre la figure 11, le bloc B1 brut comporte une première zone B1Z1 utile dont le code exécutable s'exécute et utilise les données d'application nécessaires à ladite exécution. A la fin de l'exécution dudit code, un premier lien B1L1 permet de se positionner

sur une première zone D1Z1 utile du bloc D1 décrypté. Le code de ladite zone s'exécute. A la fin de l'exécution dudit code, un lien D1L1 de ladite zone D1Z1 permet de se positionner sur une deuxième zone B1Z2 utile du bloc B1 brut dont le code s'exécute et ainsi de suite. Lorsque la dernière zone utile du bloc B1 brut s'exécute, un lien permet de charger en mémoire 41 de l'ordinateur les blocs ou pistes de données dont le logiciel d'application a besoin. Ainsi un ou plusieurs autres couples de pistes ou de blocs, brut et décrypté, sont lus et chargés en mémoire 41. Ainsi, d'après ce qui précède, il sera très difficile pour un fraudeur de reconstituer le code exécutable.

On notera que, selon le disque optique 10 de l'invention, comprenant un cryptoprocesseur, décrit précédemment, le lecteur 30 pourra comprendre un service de décryptage. On enverra ainsi des données de l'ordinateur 40 vers le cryptoprocesseur 21 du média 10 afin qu'elles soient décryptées. Ce service sera utile pour certaines architectures de sécurité dans lesquelles le logiciel d'application aurait à décrypter des parties de pistes durant l'exécution dudit logiciel.

L'invention décrite ci-dessus présente d'autres avantages décrits ci-après. L'invention présente l'avantage de pouvoir, d'une part, sécuriser des applications écrites dans un langage de haut niveau, et d'autre part, de permettre une gestion de nombreuses applications. A cette fin, le disque optique 10 comporte des données DATA formant au moins une application écrite en langage de haut niveau, notamment en langage JAVA (marque déposée). Lesdites applications sont préférentiellement cryptées en totalité ou partiellement. Ainsi, lesdites applications sont sécurisées comme décrit précédemment et ne pourront pas être dupliquées. Par ailleurs, le disque optique étant d'une grande capacité mémoire, on pourra gérer un grand nombre d'applications. Ainsi il permettra à un fournisseur d'applications de faire la promotion de ses applications et de les distribuer en masse.

Avantageusement, le disque optique est accessible en lecture-écriture pour un fournisseur d'applications. Par suite, le fournisseur pourra gérer lui-même les applications sur le disque optique à tout moment. Par exemple, à un point de vente, le fournisseur pourra télécharger des applications dans un disque à partir d'un de ses ordinateurs ou serveurs.

Le disque optique selon l'invention présente un intérêt particulier dans le domaine de la téléphonie mobile. Un mobile comporte une carte à puce de téléphonie appelée couramment carte SIM. Selon un état connu de la technique, lorsqu'un utilisateur du mobile veut utiliser un service d'un opérateur, soit l'application relative audit service se trouve sur son mobile, soit elle doit être téléchargée, dans la carte SIM, à partir d'un serveur de l'opérateur au travers d'un réseau géré par ledit opérateur. Souvent, l'opérateur propose de nouveaux services, par exemple un service de téléphonie bancaire, aux utilisateurs dont les applications doivent être téléchargées. Les applications sont généralement écrites en JAVA afin de pouvoir être modifiées et gérées par l'opérateur. Le téléchargement est long, peu fiable et le réseau est souvent encombré. De plus, la carte SIM a une mémoire réduite et ne peut supporter toutes les applications proposées par l'opérateur. Grâce au disque optique selon l'invention, un opérateur peut distribuer ses applications aux utilisateurs de manière sécurisée et évite l'encombrement de son réseau et une surcharge de la mémoire de la carte SIM. L'utilisateur achète un disque optique comportant les applications relatives aux services dont il a besoin. Il lui suffit par la suite d'insérer dans son ordinateur le disque optique et sa carte SIM dans un lecteur de carte connecté à son ordinateur et de choisir l'application qu'il souhaite charger dans sa carte. On pourra prévoir que le disque optique ne sera accessible qu'en lecture par l'utilisateur afin d'éviter qu'il ne modifie certaines données des applications.

REVENDICATIONS

1 – Disque optique sécurisé (10) de stockage de données, caractérisé en ce qu'il comporte, d'une part, un objet (20) portatif comportant une mémoire (22) comprenant au moins une clef (K1) secrète, et, d'autre part, des moyens d'échange de données, ladite clef (K1) permettant de décrypter des données (DATA) dudit disque tout en demeurant dans ledit objet portatif (20), lesdits moyens d'échange (IN_A, OUT_A, VCC_A, GRD_A) permettant d'échanger lesdites données entre ledit objet portatif et ledit disque.

2 – Disque optique selon la revendication 1, caractérisé en ce que ledit objet portatif est une puce à circuit intégré.

3 – Disque optique selon l'une des revendications précédentes, caractérisé en ce que ledit objet portatif est intégré dans une zone centrale dudit disque (10).

4 - Disque optique selon l'une des revendications précédentes, caractérisé en ce que les moyens (IN_A, OUT_A, VCC_A, GRD_A) d'échange de données sont intégrés au disque (10) au niveau d'une zone centrale.

5 - Disque optique selon l'une des revendications précédentes, caractérisé en ce qu'il comporte des moyens (E) d'équilibrage permettant d'équilibrer ledit disque.

6 - Disque optique selon l'une des revendications précédentes, caractérisé en ce que les moyens d'échange de données intégrés audit disque (10) sont avec contacts.

7 - Disque optique selon l'une des revendications 1 à 5, caractérisé en ce que les moyens d'échange de données intégrés audit disque (10) sont sans contacts.

8 - Disque optique selon l'une des revendications précédentes, caractérisé en ce que les données (DATA) sont décryptées au moyen d'un cryptoprocesseur.

9 - Disque optique selon la revendication 8, caractérisé en ce que ledit cryptoprocesseur est intégré audit objet portatif (20).

10 - Disque optique selon la revendication 8, caractérisé en ce que les données (DATA) sont modifiées au préalable en un format compréhensible par le cryptoprocesseur grâce à une interface cryptoprocesseur (37) comprise dans un lecteur de disque optique.

11 - Disque optique selon la revendication 8, caractérisé en ce que les données (DATA) sont modifiées au préalable en un format compréhensible par le cryptoprocesseur grâce à une interface cryptoprocesseur comprise dans un ordinateur (40).

12 - Disque optique selon l'une des revendications 1 à 11, caractérisé en ce que des données (DATA) du disque sont destinées à être décryptées systématiquement, qu'elles soient à l'origine cryptées ou non.

13 – Disque optique selon l'une des revendications 1 à 12, caractérisé en ce qu'un ensemble de données brutes (B) et un ensemble de données décryptées (D) ayant pour même origine un ensemble de données lues dans le disque (10) sont destinés à être envoyés à un ordinateur (40).

14 – Disque optique selon la revendication 13, caractérisé en ce qu'un ensemble de données brutes (B) est composé d'au moins une zone de données cryptées inutilisables (Bb), et, un ensemble de données décryptées (D) est composé d'au moins une zone de données décryptées utiles (Da).

15 – Disque optique selon les revendications 14 ou 15, caractérisé en ce qu'un ensemble de données brutes (B) est composé d'au

moins une zone de données non cryptées utiles (Ba), et, un ensemble de données décryptées (D) est composé d'au moins une zone de données décryptées inutilisables (Dd).

16 – Disque optique selon les revendications 13 ou 14, caractérisé en ce qu'une zone de données utiles comporte une partie de code exécutable et des données d'applications.

17 – Disque optique selon la revendication 16, caractérisé en ce que le code exécutable comprend un ensemble de liens permettant de relier différentes zones de données entre elles, de charger de nouvelles données en mémoire, de reconstituer une zone de données.

18 - Disque optique selon l'une des revendications 1 à 17, caractérisé en ce que des données (DATA) du disque forment au moins une application écrite en langage de haut niveau.

19 - Disque optique selon la revendication 18, caractérisé en ce que l'application est cryptée partiellement ou totalement.

20 - Procédé de sécurisation d'un disque optique (10) de stockage de données, caractérisé en ce que le procédé comporte les étapes selon lesquelles :

- on décrypte des données (DATA) dudit disque (10) au moyen d'une clef (K1) secrète comprise dans une mémoire (22) d'un objet (20) portatif intégré audit disque et demeurant dans ledit objet lors du décryptage,
- on échange les données (DATA) dudit disque (10) entre ledit objet portatif (20) et ledit disque grâce à des moyens (IN_A, OUT_A, VCC_A, GRD_A) d'échange de données intégrés audit disque.

21 - Procédé selon la revendication 20, caractérisé en ce que ledit objet portatif est une puce à circuit intégré.

22 - Procédé selon l'une des revendications 20 ou 21, caractérisé en ce que l'étape de décryptage est faîte au moyen d'un cryptoprocesseur intégré audit objet portatif (20).

23 - Procédé selon la revendication 22, caractérisé en ce qu'il comporte une étape supplémentaire selon laquelle :

- on modifie préalablement à l'étape de décryptage, les données (DATA) en un format compréhensible par le cryptoprocesseur grâce à une interface cryptoprocesseur (37) comprise dans un lecteur de disque optique.

24 - Procédé selon la revendication 22, caractérisé en ce qu'il comporte une étape supplémentaire selon laquelle :

- on modifie préalablement à l'étape de décryptage, les données (DATA) en un format compréhensible par le cryptoprocesseur grâce à une interface cryptoprocesseur (37) comprise dans un ordinateur (40).

25 - Procédé selon l'une des revendications 20 à 24, caractérisé en ce que, dans l'étape de décryptage, les données (DATA) sont décryptées systématiquement, qu'elles soient à l'origine cryptées ou non.

26 - Procédé selon l'une des revendications 20 à 25, caractérisé en ce qu'il comporte une étape supplémentaire selon laquelle :

- on charge dans un ordinateur (40), un ensemble de données brutes (B) et un ensemble de données décryptées (D) ayant pour même origine un ensemble de données lues dans le disque (10).

27 - Procédé selon la revendication 26, caractérisé en ce que le chargement ce fait de manière alternatif.

28 - Procédé selon la revendication 26, caractérisé en ce qu'un ensemble de données brutes (B) est composé d'au moins une zone de données cryptées inutilisables (Bb), et, un ensemble de

données décryptées (D) est composé d'au moins une zone de données décryptées utiles (Da).

29 - Procédé selon la revendication 26, caractérisé en ce qu'un ensemble de données brutes (B) est composé d'au moins une zone de données non cryptées utiles (Ba), et, un ensemble de données décryptées (D) est composé d'au moins une zone de données décryptées inutilisables (Dd).

30 - Procédé selon les revendications 28 ou 29, caractérisé en ce qu'il comporte une étape supplémentaire selon laquelle :

- on exécute une partie de code exécutable compris dans une zone de données utiles comprenant des données d'applications.

31 - Procédé selon la revendication 30, caractérisé en ce qu'il comporte une étape supplémentaire selon laquelle :

- on relie différentes zones de données entre elle, on charge de nouvelles données en mémoire, on reconstitue une zone de données au moyen d'un ensemble de liens compris dans le code exécutable.

32 - Procédé selon l'une quelconque des revendications 20 à 31, caractérisé en ce qu'il comporte une étape supplémentaire selon laquelle :

- on crypte des données au moyen d'une clef (K1) secrète,
- on inscrit lesdites données cryptées dans ledit disque (10).

33 - Procédé selon l'une quelconque des revendications 20 à 32, caractérisé en ce qu'il comporte des données (DATA) formant au moins une application écrite en langage de haut niveau.

34 - Procédé selon la revendication 33, caractérisé en ce que l'application est cryptée partiellement ou totalement.

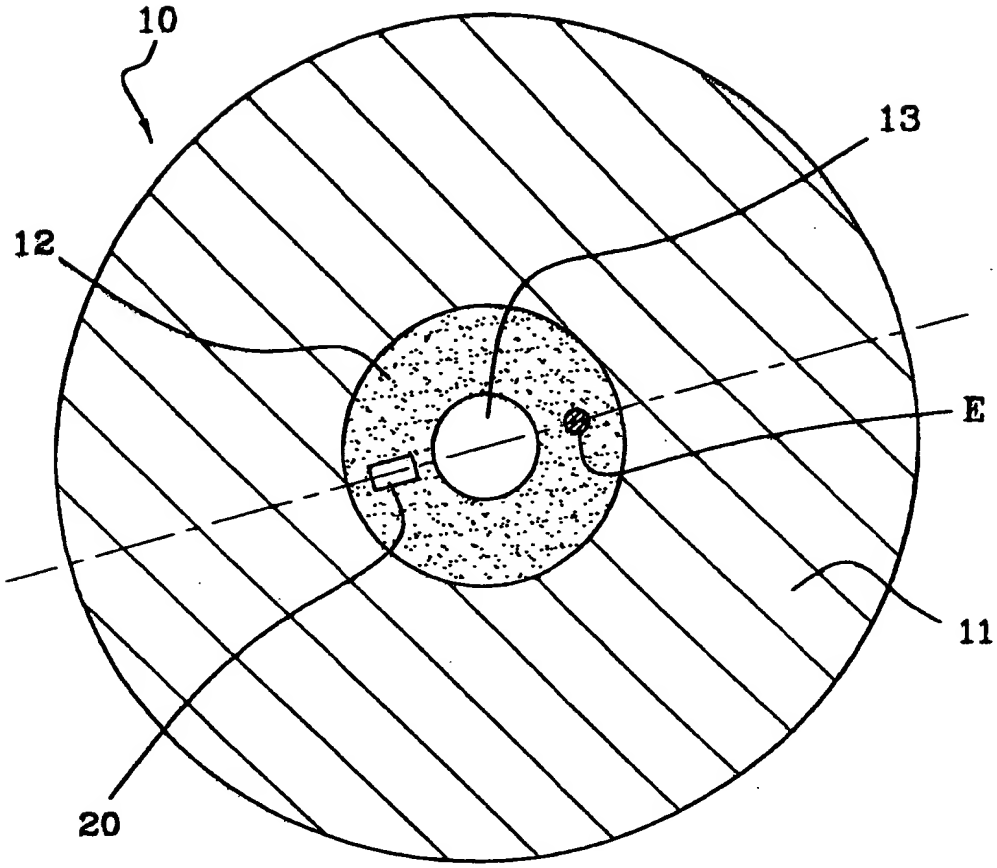


FIG.1

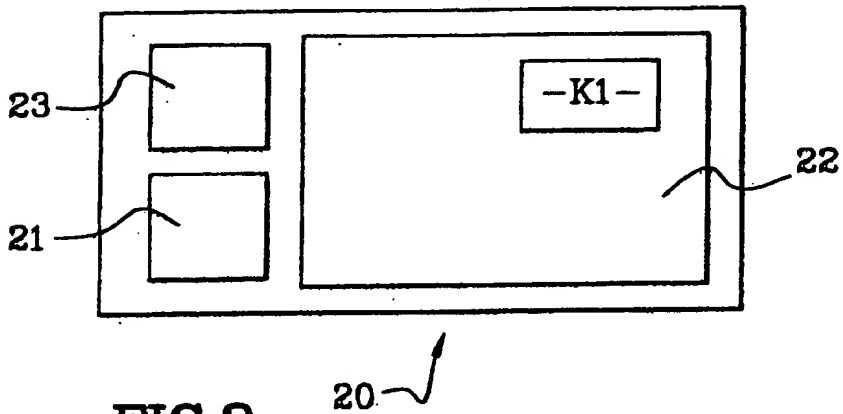


FIG.2

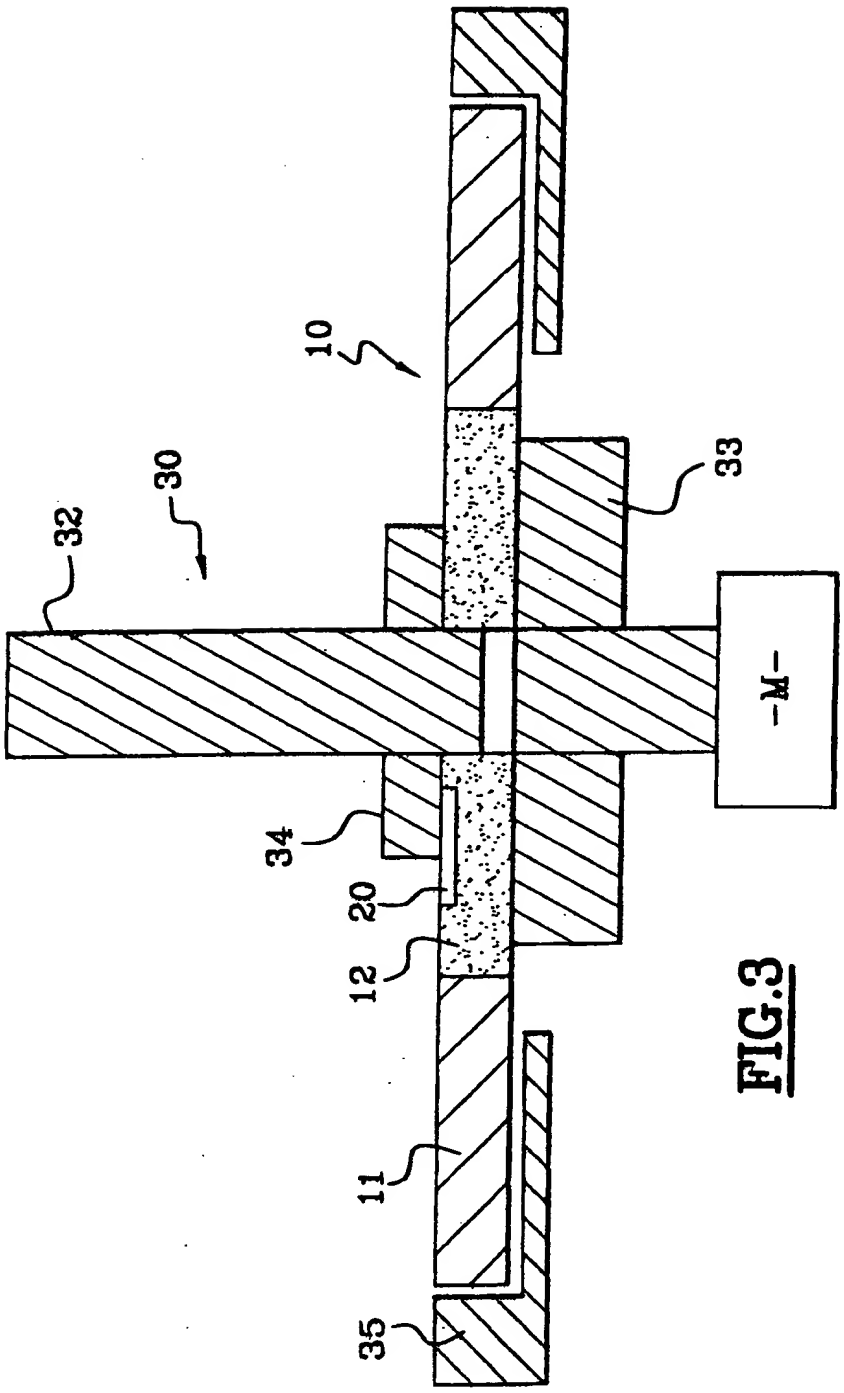


FIG.3

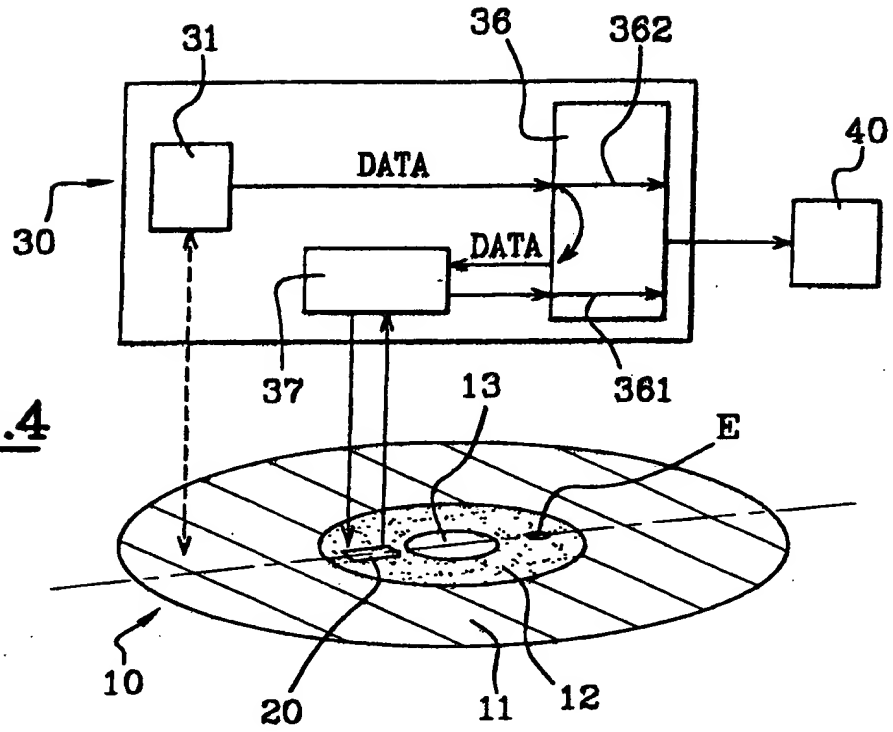

31
36
362
40
DATA
30
DATA
37
13
361
E
10
20
11
12

FIG.4

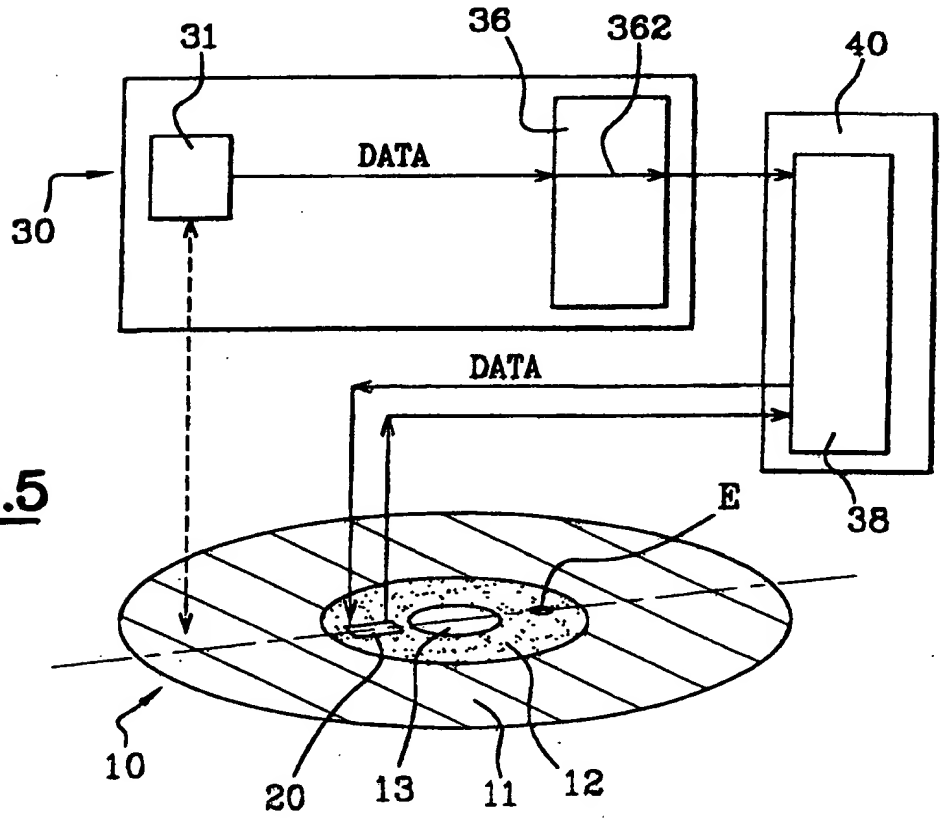

31
36
362
40
DATA
30
DATA
E
38
10
20
13
11
12

FIG.5

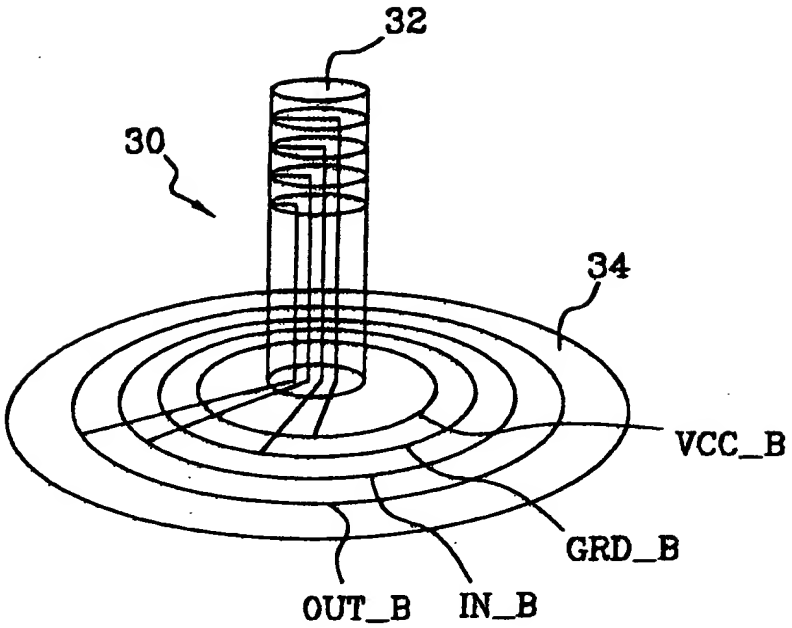

32
30
34
VCC_B
GRD_B
OUT_B
IN_B

FIG.6

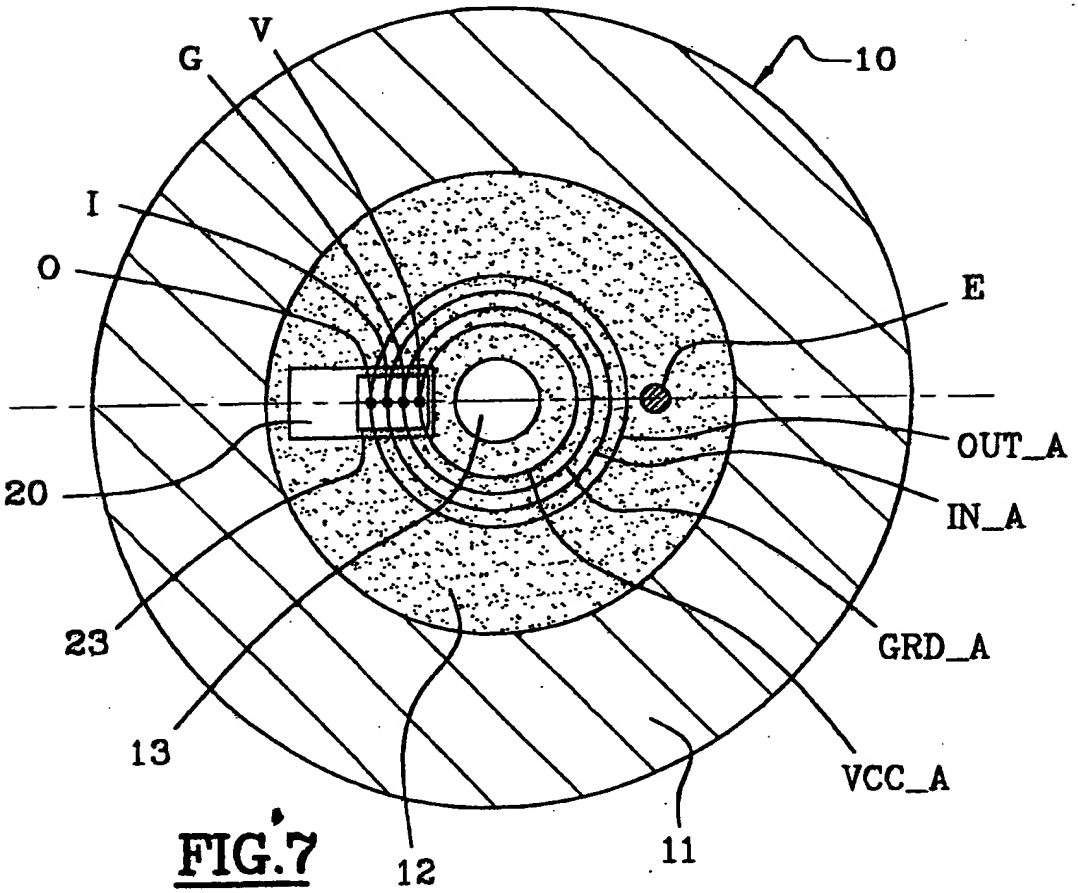

V
G
10
I
O
E
OUT_A
20
IN_A
23
GRD_A
13
VCC_A
12
11

FIG.7

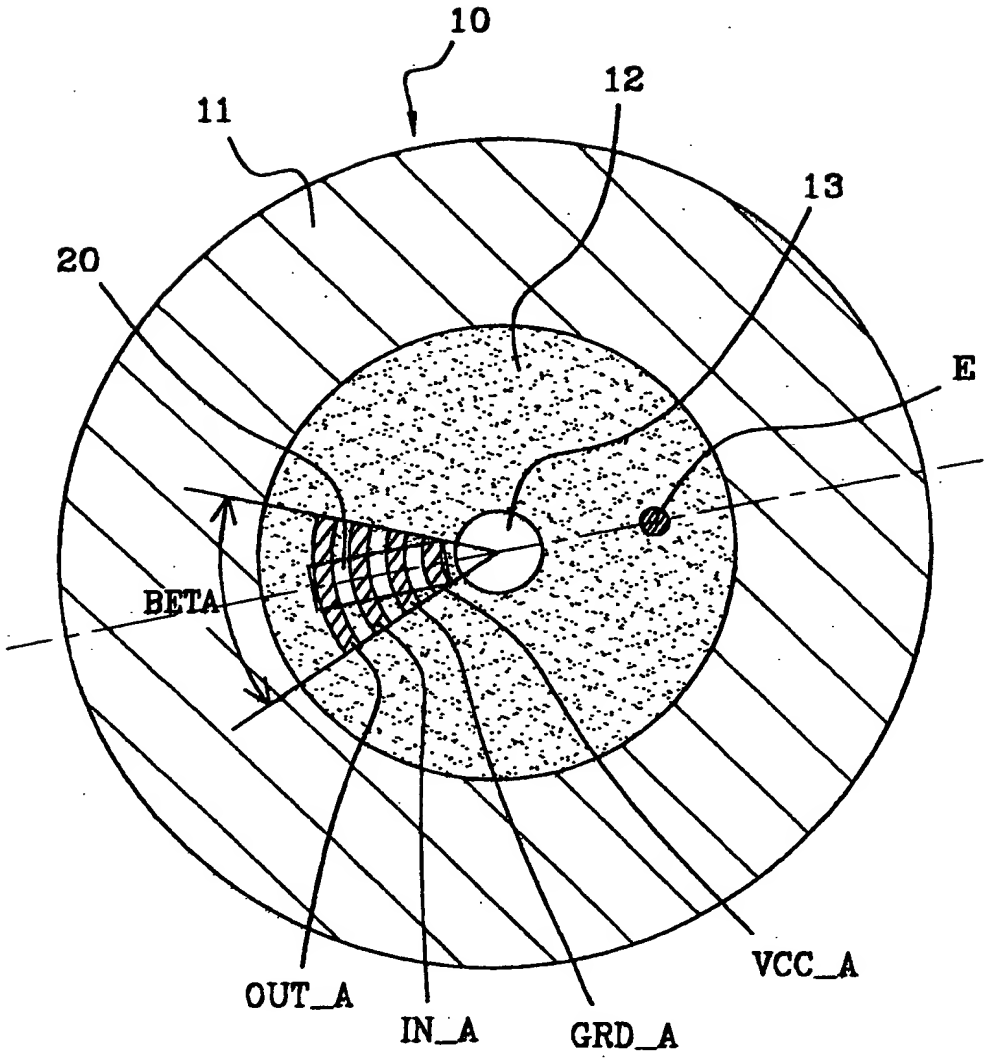


FIG.8

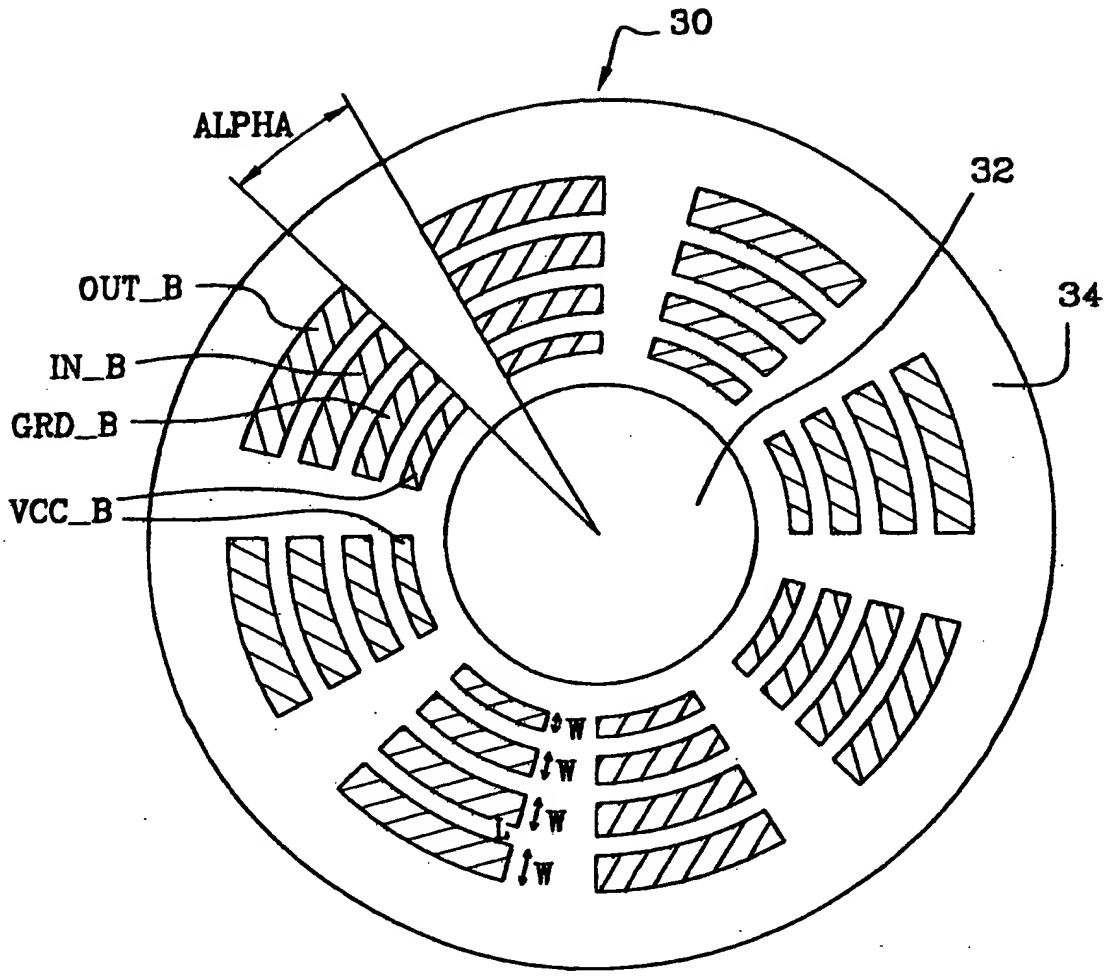


FIG.9

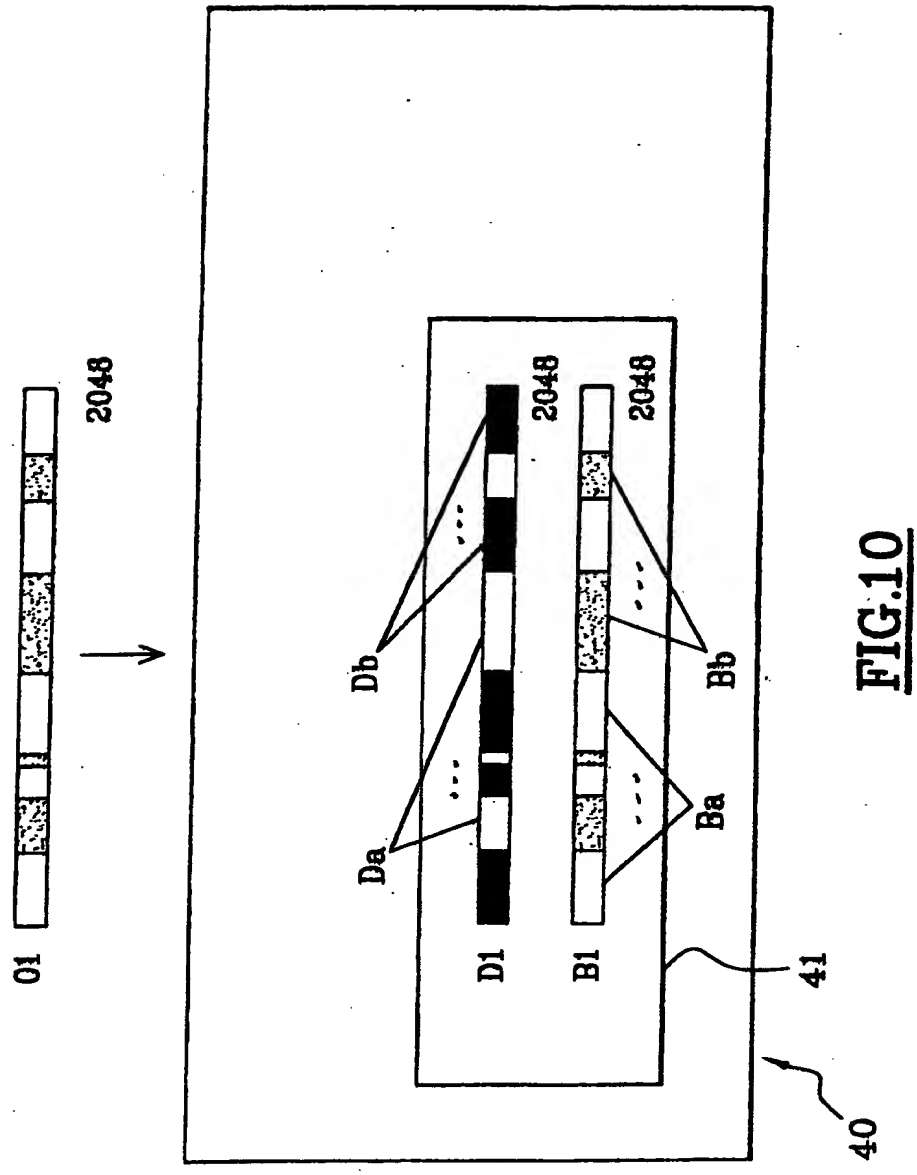


FIG.10

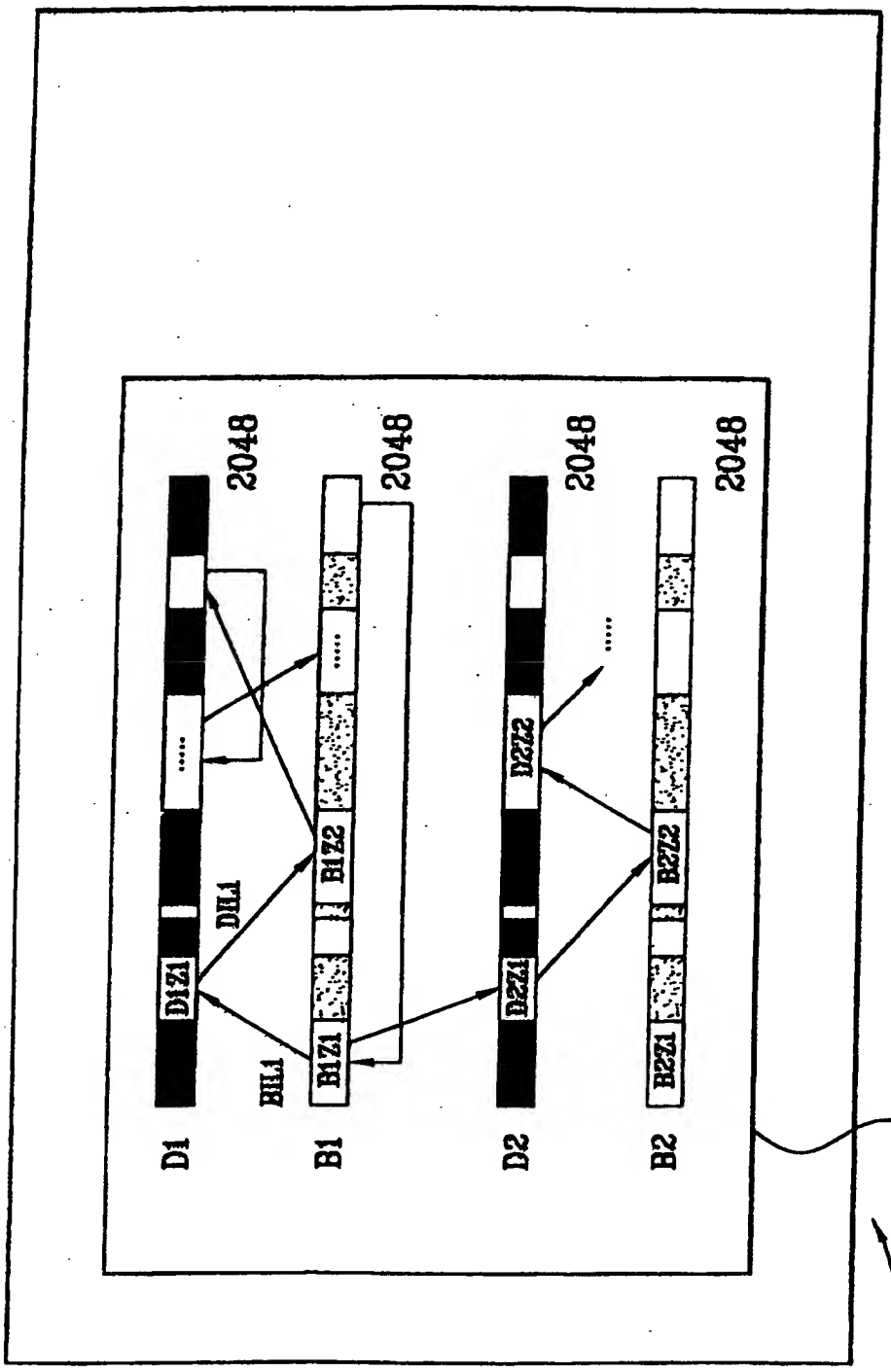

2048
2048
2048
2048
D1Z1
DIL1
B1Z2
B1Z1
BIL1
D2Z2
D2Z1
B2Z2
B2Z1
D1
B1
D2
B2
41
40

FIG.11

INTERNATIONAL SEARCH REPORT

Inte. ational Application No
PCT/FR 00/00483

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 G11B23/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DE 42 42 247 A (ORGA KARTENSYSTEME GMBH) 16 June 1994 (1994-06-16) abstract column 1, line 3 - line 18 column 2, line 23 - line 41 column 2, line 46 -column 3, line 60 figures 1,3	1-4,7-9, 18-22, 32-34
Y	EP 0 849 734 A (TEXAS INSTRUMENTS INC) 24 June 1998 (1998-06-24) abstract column 2, line 22 - line 34 column 3, line 32 - line 58 figure 1	1-4,7-9, 18-22, 32-34

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 April 2000	04/05/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Barel-Faucheux, C

2

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	FR 2 643 475 A (LIVOWSKY JEAN MICHEL) 24 August 1990 (1990-08-24) abstract page 10, line 18 - line 32 page 14, line 1 - line 15 figure 3	1,8,9
A	EP 0 774 706 A (DEUTSCHE TELEKOM AG) 21 May 1997 (1997-05-21) abstract column 1, line 52 -column 4, line 4 figure 1	1,6
A	EP 0 809 245 A (TEXAS INSTRUMENTS INC) 26 November 1997 (1997-11-26) abstract	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte. ional Application No
PCT/FR 00/00483

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 4242247 A	16-06-1994	NONE	
EP 0849734 A	24-06-1998	JP 10228727 A	25-08-1998
FR 2643475 A	24-08-1990	AU 5173790 A	26-09-1990
		DD 292987 A	14-08-1991
		WO 9010292 A	07-09-1990
		GR 90100111 A	28-06-1991
EP 0774706 A	21-05-1997	DE 19542910 A	22-05-1997
		CA 2190437 A	18-05-1997
		NO 964835 A	20-05-1997
		US 5881152 A	09-03-1999
EP 0809245 A	26-11-1997	JP 10075198 A	17-03-1998
		US 5905798 A	18-05-1999

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 00/00483

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G11B20/00 G11B23/28

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G11B

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relevent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	DE 42 42 247 A (ORGA KARTENSYSTEME GMBH) 16 juin 1994 (1994-06-16) abrégé colonne 1, ligne 3 - ligne 18 colonne 2, ligne 23 - ligne 41 colonne 2, ligne 46 -colonne 3, ligne 60 figures 1,3	1-4,7-9, 18-22, 32-34
Y	EP 0 849 734 A (TEXAS INSTRUMENTS INC) 24 juin 1998 (1998-06-24) abrégé colonne 2, ligne 22 - ligne 34 colonne 3, ligne 32 - ligne 58 figure 1	1-4,7-9, 18-22, 32-34

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
26 avril 2000	04/05/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Barel-Faucheux, C

2

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	FR 2 643 475 A (LIVOWSKY JEAN MICHEL) 24 août 1990 (1990-08-24) abrégé page 10, ligne 18 - ligne 32 page 14, ligne 1 - ligne 15 figure 3	1,8,9
A	EP 0 774 706 A (DEUTSCHE TELEKOM AG) 21 mai 1997 (1997-05-21) abrégé colonne 1, ligne 52 -colonne 4, ligne 4 figure 1	1,6
A	EP 0 809 245 A (TEXAS INSTRUMENTS INC) 26 novembre 1997 (1997-11-26) abrégé	1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Den. de internationale No
PCT/FR 00/00483

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
DE 4242247 A	16-06-1994	AUCUN	
EP 0849734 A	24-06-1998	JP 10228727 A	25-08-1998
FR 2643475 A	24-08-1990	AU 5173790 A	26-09-1990
		DD 292987 A	14-08-1991
		WO 9010292 A	07-09-1990
		GR 90100111 A	28-06-1991
EP 0774706 A	21-05-1997	DE 19542910 A	22-05-1997
		CA 2190437 A	18-05-1997
		NO 964835 A	20-05-1997
		US 5881152 A	09-03-1999
EP 0809245 A	26-11-1997	JP 10075198 A	17-03-1998
		US 5905798 A	18-05-1999